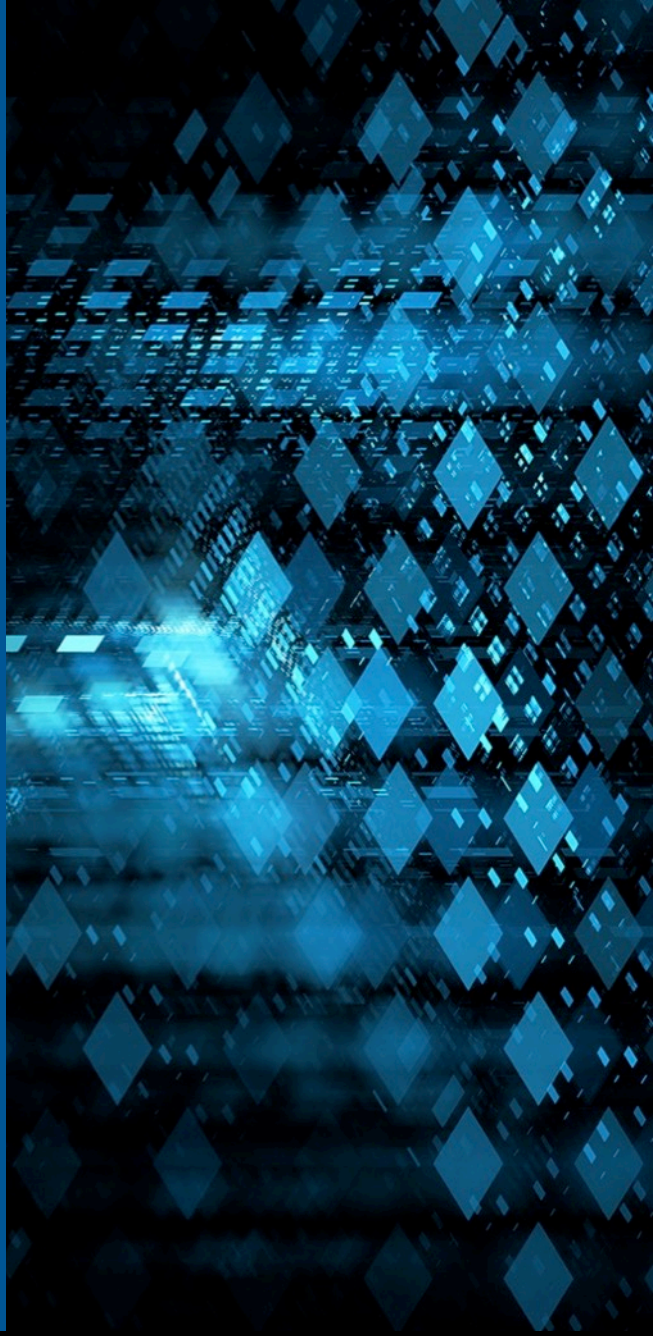
Real-world Cases of Insider Threat: Combating Malicious IT Insiders

Craig Lewis, SEI

Joe Tammariello, SEI

Rich Voninski, Splunk

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Distribution Statements

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material was prepared for the exclusive use of Splunk Conference and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0535

About the speakers

Craig Lewis (SEI)

- Speaking to actual insider threat cases

Joe Tammariello (SEI)

- Using Splunk to help identify concealment methods

Rich Voninski (Splunk)

- Integrating the *Audit the Auditors* app

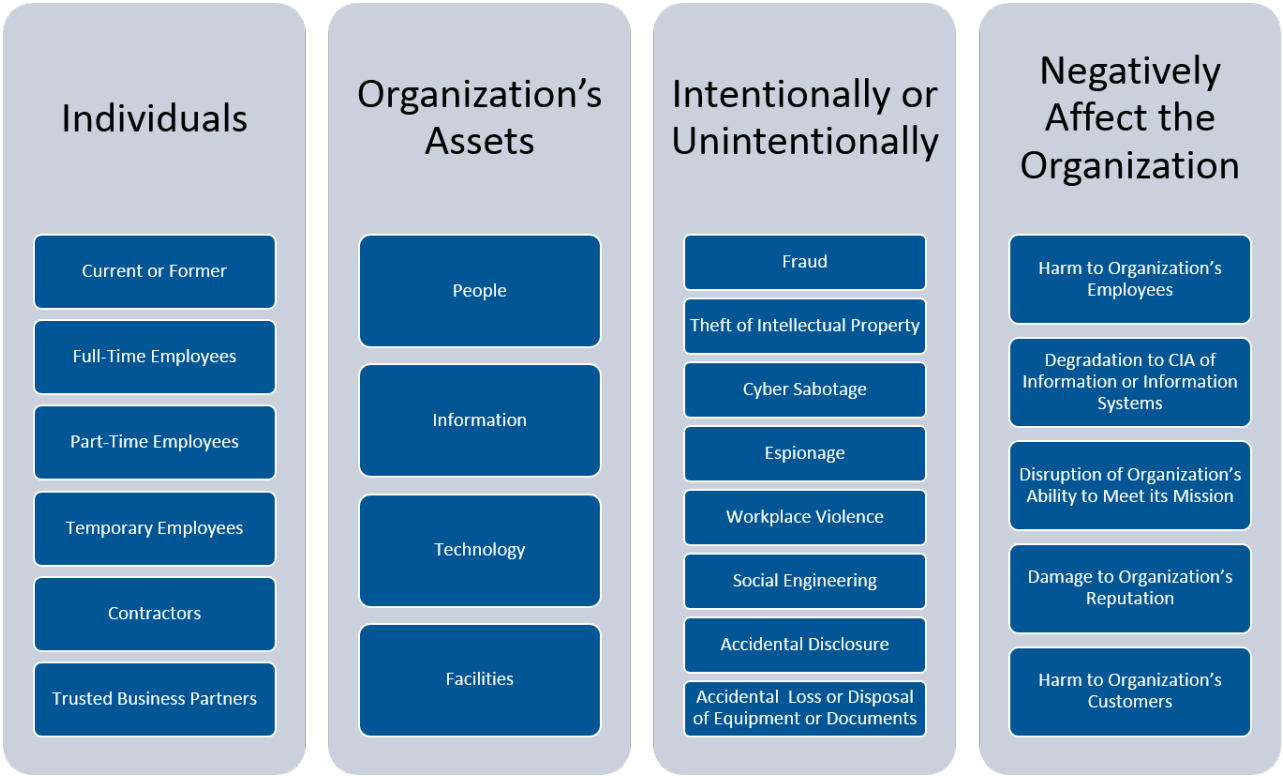
The CERT Insider Threat Center

The CERT Insider Threat Center is a Center of Insider Threat Expertise at the Software Engineering Institute

- Began working in this area in 2001 with the U.S. Secret Service
- Mission: Enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats
- Action and Value: Conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

What is an Insider Threat?

Insider Threat: the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.



Why Insider Threat is Important

It's an organizational risk

- In surveys[1] analyzed in SEI/CERT and CSO Magazine report:
  - 47% of survey participants reported an insider incident
  - 27% of attacks against their orgs were committed by insiders
  - About one-third of participants could not identify the individual(s) behind the attack
    - A quarter **did not have enough information** to take legal action

You may have requirements related to Insider Threat

- National Industrial Security Program Operating Manual – Change 2
- DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - From the NIST 800-171 rev. 1

  3.2.3 *Provide security awareness training on recognizing and reporting potential indicators of insider threat*[2]

[1] https://insights.sei.cmu.edu/insider-threat/2017/01/2016-us-state-of-cybercrime-highlights.html
[2] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Covering the basics is good

How to get caught 101:

- The smash and grab
  - Large data uploads
  - Increased email leaving the organization
  - Massive file collection or print jobs

- Abnormal access
  - Change in work hours or locations
  - Hitting systems one normally doesn't

Account lifecycle:

- You would be amazed at the number of cases where access is gained using accounts that **remained active** after separation

What about IT folks who have all the keys?

This talk seeks to explore a specific subset of insider threat:

Insider threat

- -Unintentional
- -Intentional
  - -Unprivileged
  - **-Privileged (IT etc.)**
    - **-Concealment Efforts**

These are the folks who know where the ‘security cameras’ are!

Case Studies

Insider Threat Database

Using the Insider Threat Database

The Insider Threat Database contains actual cases of insider threat activities

- Leverage these cases to think about what people *really* have done rather than purely hypothetical

Scenario #1 – Going after the logs

Case A:

- A systems administrator working as a contractor for a government agency made false statements in order to gain employment
- Worked for approximately 3 years before attack
- Stole data from classified and unclassified systems

Concealment:

- Disabled networking on hosts and used privileged access to disable application that would have been centrally collected logs

Scenario #1 – Going after the logs

Case B:

- Insider was one of two network administrators and was envious of co-administrator's position as supervisor
- Took advantage of "network problems" to plant logic bomb and modify files to frame the co-administrator
- Insider produced logs they had tampered with as evidence that the co-administrator was guilty
- Co-administrator was suspended and later fired. Deeper investigation uncovered inconsistencies. Insider later fired though not prosecuted

Concealment: Modification of logging. Using downtime to prevent incriminating events from being recorded.

Scenario #1 – Going after the logs

So let's explore the concealment:

- Do we know we're getting the logs we need?
- Did any nodes go dark?
- Are all the data in Splunk?
  - Or were some…deleted??

Scenario #1 – Going after the logs

To Splunk!

- **Can_Delete Role Mapping (alert and sound air horn)**
  - | rest /servicesNS/nobody/system/admin/LDAP-groups | rename title as AD_Group | table AD_Group, roles | search roles=can_delete

AD_Group	roles
Splunk.Delete	can_delete

- **Roles with Delete_By_Keyword Capability (alert and sound air horn)**
  - | rest services/authorization/roles | search title!=can_delete capabilities=delete_by_keyword | rename title AS role_with_delete | table capabilities, role_with_delete | sort-_time

capabilities	role_with_delete
delete_by_keyword	proxy
schedule_rtsearch	

Scenario #1 – Going after the logs

- **Role Modification (See who caused the previous Alerts)**
  - index=_internal sourcetype=splunkd_ui_access action=edit uri=*authorization/roles* OR uri=*LDAP-groups* NOT StreamedSearch | table _time, user, clientip, action, file, user_watchlist | sort -_time

_time	user	clientip	action	file	user_watchlist
2017-07-17 14:35:08.957	ria_mui	00.60.3.60	edit	LDAP-groups	false
2017-07-17 14:35:04.715	ria_mui	00.60.3.60	edit	Splunk.Delete	false
2017-07-17 14:35:01.501	ria_mui	00.60.3.60	edit	Splunk.Delete	false
2017-07-17 14:34:18.772	ria_mui	00.60.3.60	edit	LDAP-groups	false
2017-07-17 14:34:15.121	ria_mui	00.60.3.60	edit	Splunk.Delete	false
2017-07-17 14:34:08.564	ria_mui	00.60.3.60	edit	Splunk.Delete	false
2017-07-17 14:32:44.690	ria_mui	00.60.3.60	edit	proxy	false
2017-07-17 14:32:43.025	ria_mui	00.60.3.60	edit	roles	false
2017-07-17 14:32:39.951	ria_mui	00.60.3.60	edit	proxy	false

Scenario #1 – Going after the logs

- **Gaps in Logging (We know we send Perfmon data every 15 minutes)**
  - sourcetype=Perfmon* earliest=-90m |streamstats current=f last(_time) as last_time by host | eval gap = last_time - _time | convert ctime(last_time) as last_time | search gap>915 | eval gap=gap/60 | rename gap as minutes_since_last_perfmon | table _time, last_time, minutes_since_last_perfmon, host

_time	last_time	minutes_since_last_perfmon
2017-07-21 07:35:32	07/21/2017 08:02:09	26.616667

- **Security Event Log Cleared**
  - index=wineventlog host=* LogName=Security EventCode=1102 | table _time, host, Account_Name, Message, user_watchlist | sort-_time

_time	host	Account_Name	Message	user_watchlist
2017-07-12 07:57:09	prbquilunbyds	nia_bao	The audit log was cleared. Subject: Security ID: GUILLERMINA\nia_bao Account Name: nia_bao Domain Name: GUILLERMINA Logon ID: 0k01G1MD	false
2017-07-05 08:48:15	prbquilunbyds	nia_bao	The audit log was cleared. Subject: Security ID: GUILLERMINA\nia_bao Account Name: nia_bao Domain Name: GUILLERMINA Logon ID: 0f0Y0M72HX	false

Scenario #1 – Going after the logs

- **Stopped Universal Forwarder (not a maintenance period)**
  - index=wineventlog SourceName="Microsoft-Windows-Service Control Manager" SplunkForwarder | eval Time=strftime(_time,"%H") | search Time!=4 Time!=5 Time!=6 | table _time, host, Message | sort-_time

_time	host	Message
2017-07-17 15:05:26	jattestserver	The SplunkForwarder Service service entered the running state.
2017-07-17 15:05:18	jattestserver	The SplunkForwarder Service service entered the stopped state.
2017-07-17 15:05:04	jattestserver	The SplunkForwarder Service service entered the running state.
2017-07-17 15:03:27	jattestserver	The SplunkForwarder Service service entered the stopped state.

Scenario #2 – Stopping others from receiving alerts

Case:

- A systems administrator decided to attack the victim organization's network in response to a business decision made by management.
- The insider compromised email accounts and forwarded those emails externally.
- Deleted backups, VMs, emails, and other data
- Resigned before wrongdoing could be discovered

Concealment:

- Removed staff from distribution lists used for auditing and alerting

Scenario #2 – Stopping others from receiving alerts

So let's explore the concealment:

- How do you receive alerts?
- What protections are there around alerting and notification?

Scenario #2 – Stopping others from receiving alerts

To Splunk!

- **Enable/Disable Splunk Alerts (and who)**
  - index=_internal method=post "*saved/searches*" file=enable OR file=disable NOT StreamedSearch | REX "^(?:[^/\n]*/){8}(?P<search_name>[^/]+)" | rename file as action | table _time, user, action, search_name, user_watchlist

_time	user	action	search_name	user_watchlist
2017-07-17 11:30:30.165	ira_zoe	enable	can_delete	false
2017-07-17 11:30:24.631	ira_zoe	disable	can_delete	false
2017-07-17 11:30:08.789	ira_zoe	enable	NON-US%20FTR%00Cknittypvfu%20-%20Pxhni	false
2017-07-17 11:30:03.037	ira_zoe	disable	NON-US%20FTR%00Cknittypvfu%20-%20Pxhni	false
2017-07-17 11:08:50.808	ira_zoe	enable	Concepcion%20Fpfysix	false
2017-07-17 10:46:15.091	ira_zoe	disable	Concepcion%20Fpfysix	false

Scenario #2 – Stopping others from receiving alerts

- **Saved Search (or Alert) Modifications (and who)**
  - index=_internal sourcetype=splunkd_ui_access method=post "*saved/searches*" action=edit NOT StreamedSearch | rename file as search_name | table _time, user, clientip, search_name, action, user_watchlist

_time	user	clientip	search_name	action	user_watchlist
2017-07-17 11:47:02.475	don_mee	00.41.3.41	Hermelinda%1400Htqgyml	edit	false
2017-07-17 10:59:56.276	don_mee	00.41.3.41	Hermelinda%1400Htqgyml	edit	false

Scenario #2 – Stopping others from receiving alerts

- **Adding/Removing People from Distribution Lists**
  - index=* ComputerName=DOMAINCONTROLLER AND (Account_Name="Domain Admins" OR Account_Name="Enterprise Admins" OR Account_Name="Schema Admins" AND (EventCode=4728 OR EventCode=4729 OR EventCode=4732 OR EventCode=4733 OR EventCode=4756 OR EventCode=4757) | REX "was (?<action>.*).?(to|from)"| Rename user As "User Added or Removed" | Rename src_user AS "Changed By" | table _time, "User Added or Removed", action, "Changed By", Account_Name, Group_Name | sort-_time

_time	User Added or Removed	action	By	Account_Name	Group_Name
2017-07-20 08:15:07	AS=Hue Jackqueline (admin),DA=Hannah,DA=ODA Users,DH=ad,DH=oda,DH=min,DH=edu	removed	kia_sol	kia_sol AS=Hue Jackqueline (admin),DA=Hannah,DA=ODA Users,DH=ad,DH=oda,DH=min,DH=edu	Schema Hannah
2017-07-20 08:15:07	AS=Hue Test,DA=ODA,DA=IT,DA=People,DH=ad,DH=oda,DH=min,DH=edu	removed	kia_sol	kia_sol AS=Hue Test,DA=ODA,DA=IT,DA=People,DH=ad,DH=oda,DH=min,DH=edu	Schema Hannah
2017-07-20 08:15:00	AS=Hue Jackqueline (admin),DA=Hannah,DA=ODA Users,DH=ad,DH=oda,DH=min,DH=edu	added	kia_sol	kia_sol AS=Hue Jackqueline (admin),DA=Hannah,DA=ODA Users,DH=ad,DH=oda,DH=min,DH=edu Schema Hannah	
2017-07-20 08:15:00	AS=Hue Test,DA=ODA,DA=IT,DA=People,DH=ad,DH=oda,DH=min,DH=edu	added	kia_sol	kia_sol AS=Hue Test,DA=ODA,DA=IT,DA=People,DH=ad,DH=oda,DH=min,DH=edu Schema Hannah	

Scenario #2 – Stopping others from receiving alerts

- **Full Access permissions on mailboxes to delete mail**
  - index=* host=MAILSERVER sourcetype="XmlWinEventLog:MSExchange Management" modification_type=*permission*| table _time,mailbox_modified, modification, modified_by, access, modification_type,host | sort-_time

_time	mailbox_modified	modification	modified_by	access	modification_type
2017-05-12 10:10:38	ad.rey.lai.edu/People/IT/REY/Sheba Shala	plt1	Lyn Christopher (admin)	LdrhEeqmtp	Remove-EukpqppSejxzyantk
2017-05-12 10:08:26	ad.rey.lai.edu/People/IT/REY/Sheba Shala	plt1	Lyn Christopher (admin)	LdrhEeqmtp	Add-EukpqppSejxzyantk
2017-05-12 10:06:26	ad.rey.lai.edu/People/IT/REY/Lyn Christopher	plt1	Lyn Christopher (admin)	LdrhEeqmtp	Remove-EukpqppSejxzyantk
2017-05-12 09:48:26	ad.rey.lai.edu/People/IT/REY/Ivonne Ismael	dominic	Lyn Christopher (admin)	LdrhEeqmtp	Remove-EukpqppSejxzyantk
2017-05-12 09:44:44	ad.rey.lai.edu/People/IT/REY/Ivonne Ismael	dominic	Lyn Christopher (admin)	LdrhEeqmtp	Add-EukpqppSejxzyantk
2017-05-12 09:42:50	ad.rey.lai.edu/People/IT/REY/Lyn Christopher	plt1	Lyn Christopher (admin)	LdrhEeqmtp	Add-EukpqppSejxzyantk

So you *claim* your analysts are reviewing this data…

- Well, you can find out if that's true….or if any tampering has occurring on your dashboards
- Simple search to see who has edited which dashboards
  - index=_internal NOT StreamedSearch method=POST ui/views | rename file as Dashboard | table _time, user, dashboard, user_watchlist | sort-_time

_time	user	clientip	dashboard	user_watchlist
2017-07-17 11:44:36.187	pat_lia	10.10.3.10	insider_threats	false
2017-07-17 09:50:36.968	rosalind_lia	10.10.3.010	nagios	false
2017-07-17 09:49:53.264	rosalind_lia	10.10.3.010	nagios	false

Splunk App

Audit the Auditors

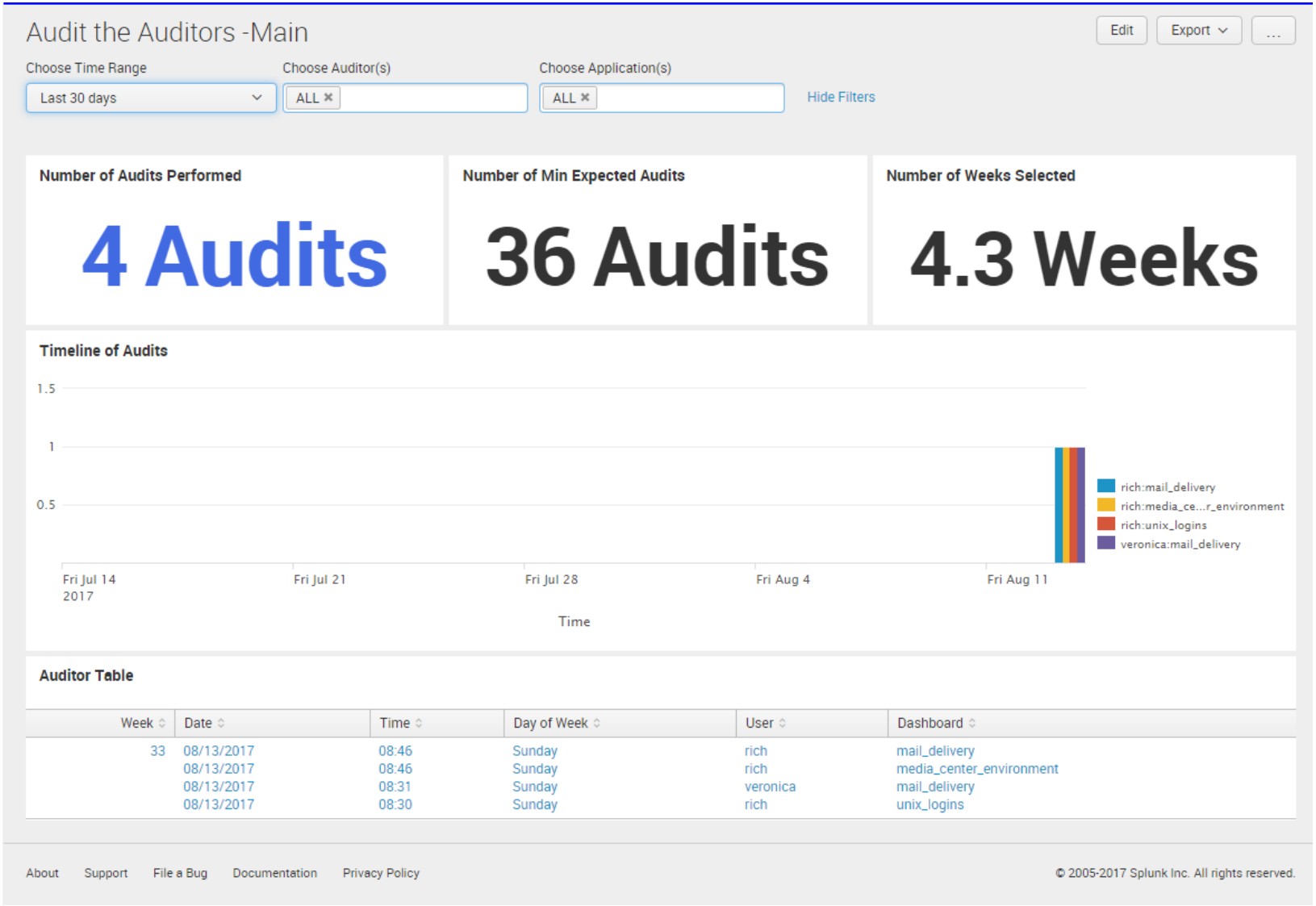
What is Audit the Auditors?

Q: “How can I verify that my team is checking the dashboards?”

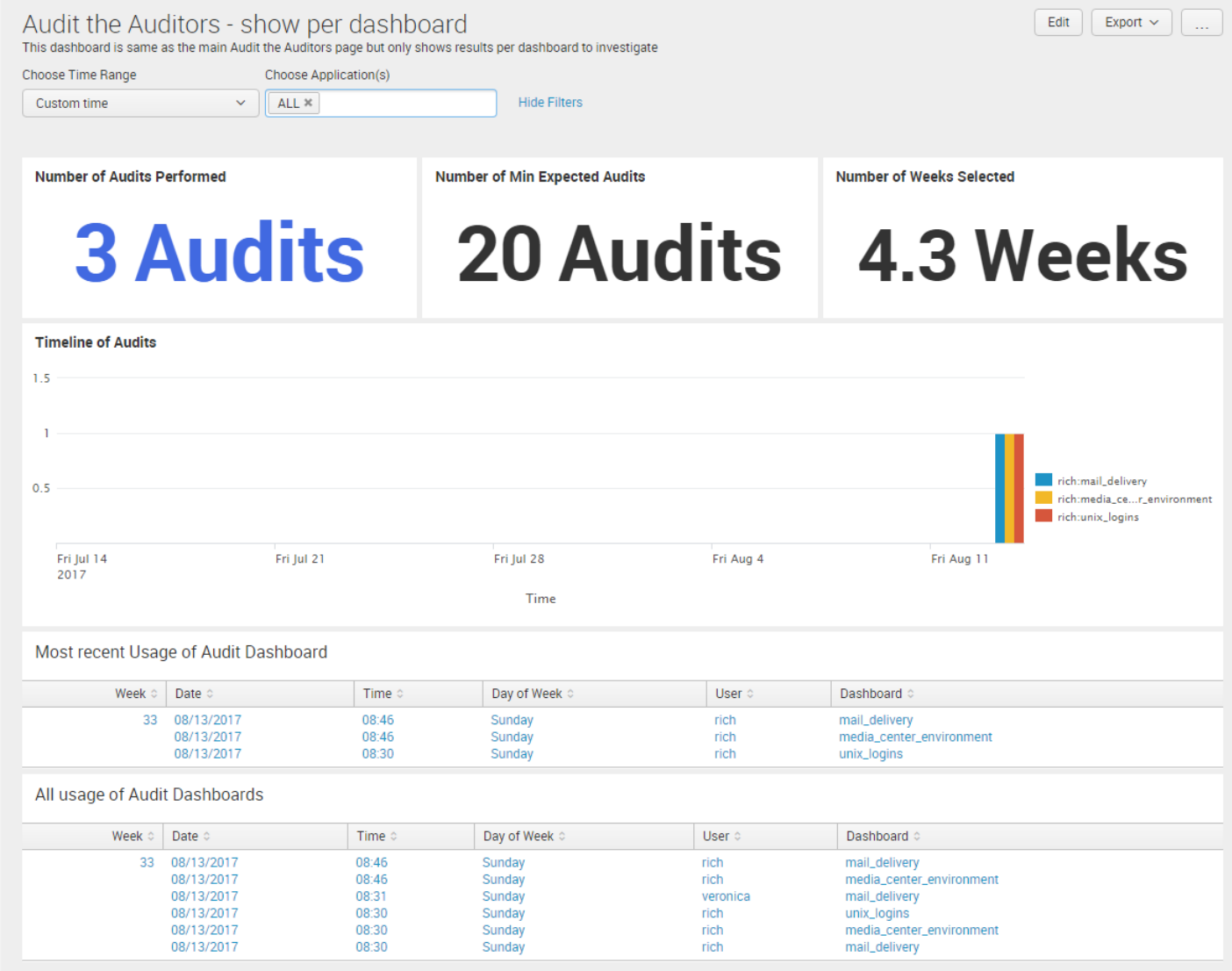
A: Audit the Auditors was born

- Application allows you to verify team is completing audits
  - Assign teammates and/or specific audit dashboards per weekly schedule
  - System reports:
    - Who last accessed ‘audit’ dashboards and when
    - Also can show full record of when specific dashboards have been accessed

Audit the Auditors – Main Page



Audit the Auditors – By Dashboard

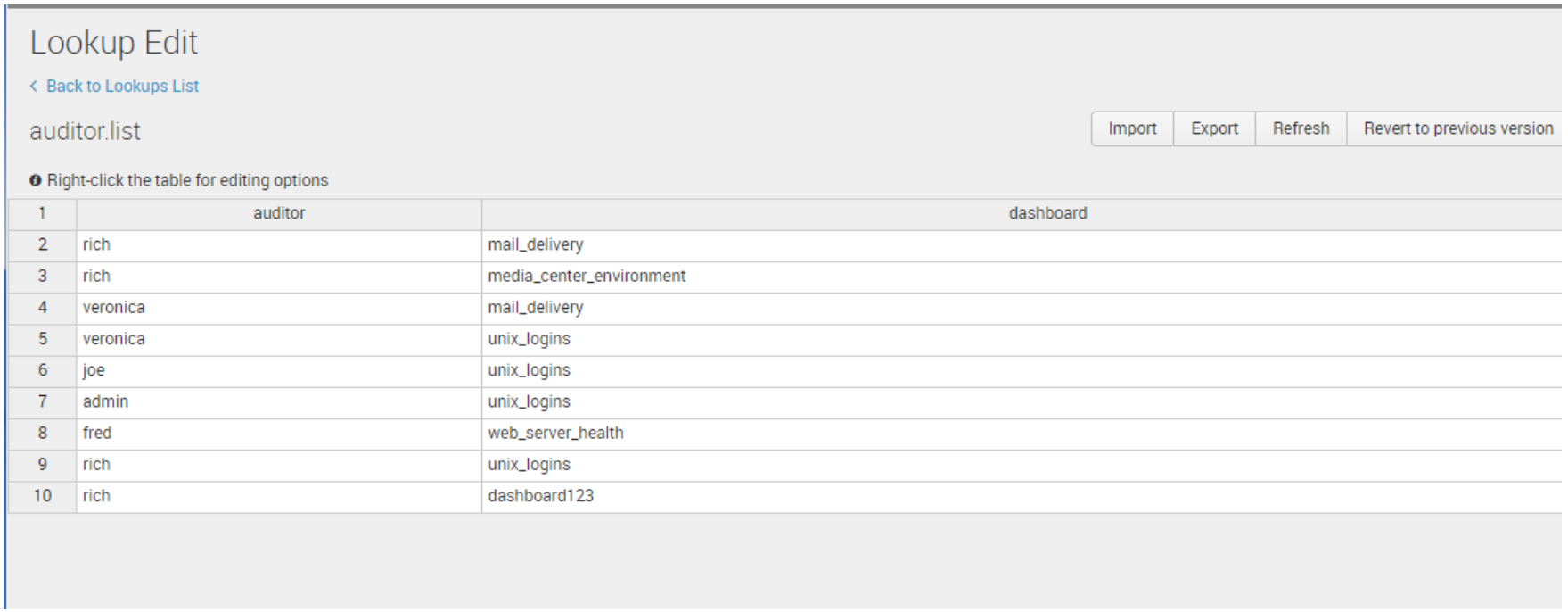


Audit the Auditors – How does it work?

- Based on *_internal* index and sourcetype *splunk_web_access*
- Utilizes lookup table to identify users and dashboards of interest
- Needs field extractions for getting to dashboard and application names
- Limitations:
  - Does not detect usage through Mobile Application
  - Current Version only gives ~30 days of audit
    - Future version will write its own data to persist

Audit the Auditors – Lookup File

- Assign user and responsibilities



Lookup Edit

< Back to Lookups List

auditor.list

Import | Export | Refresh | Revert to previous version

Right-click the table for editing options

1	auditor	dashboard
2	rich	mail_delivery
3	rich	media_center_environment
4	veronica	mail_delivery
5	veronica	unix_logins
6	joe	unix_logins
7	admin	unix_logins
8	fred	web_server_health
9	rich	unix_logins
10	rich	dashboard123

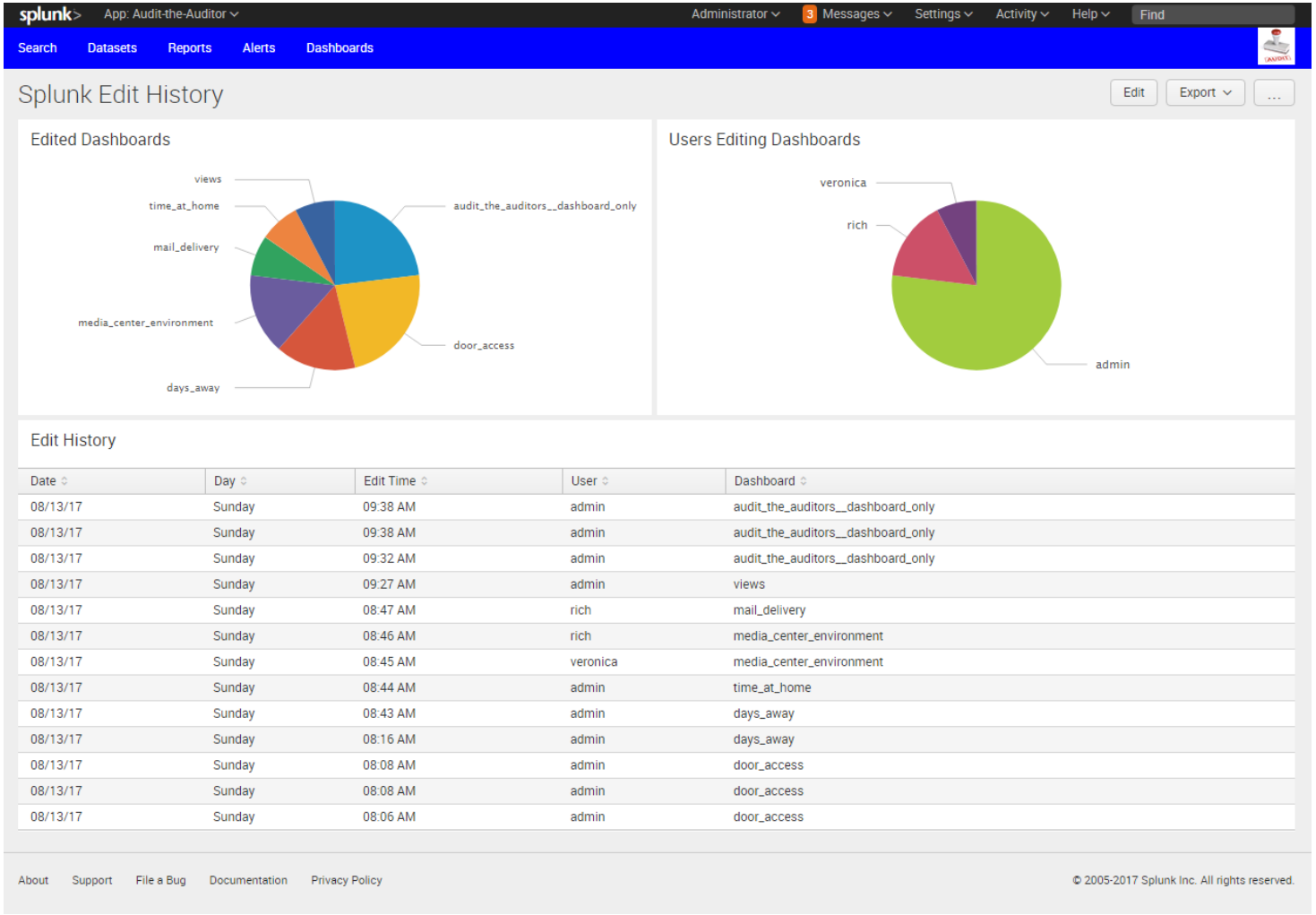
Organic Growth (suggestions added)

- "We would like to know who is using what application/dashboards?"
  - Useful for:
    - Seeing if your Splunk apps are getting traction among team
    - Seeing who is using what & when

- "How can we see if someone edited a Splunk application?"
  - Useful for:
    - Watching the watchers
    - If manually changed you need another configuration management mechanism to check file integrity
    - Utilize queries shown a few pages back

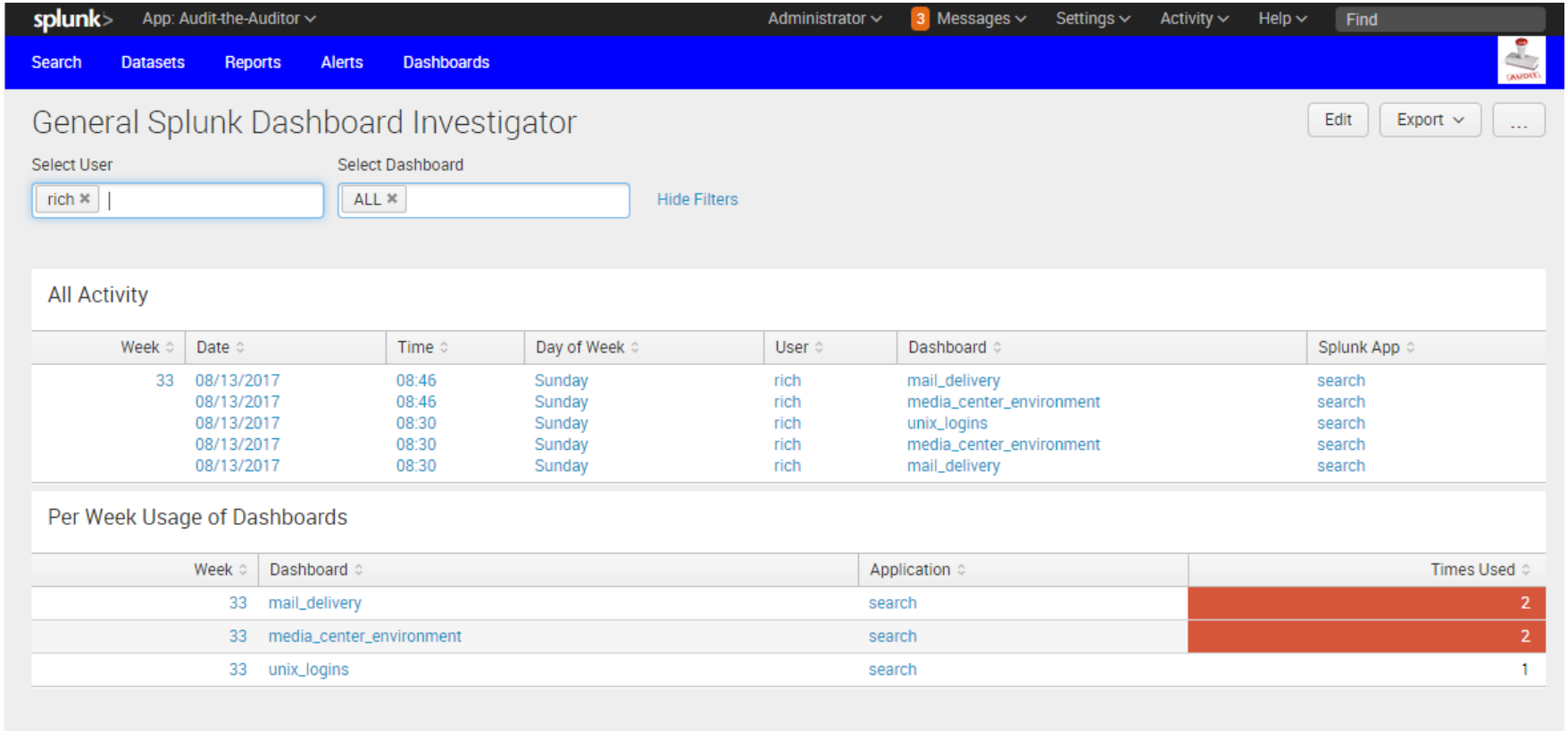
Splunk Edit History

- Built on queries and sources shown in previous section



Splunk Usage

- Specify by User or Dashboard
  - Allows you to see who has been using what and when



Audit the Auditors

- Plan to package up for Splunkbase
- Until then, if interested please email me
  - Rich Voninski – rvoninski@splunk.com

Call to Action

- Get the right people involved
  - HR, Business Services, IT systems groups, Legal, Physical Security, etc.
  - Work with your insider threat program
- Identify your critical systems
  - And make sure you are monitoring them
    - Harden your monitoring
    - Identify highly privileged IT staff members
  - Create watch list
- Audit the monitoring
  - You are asserting that you are monitoring for threats
    - Prove that you are

High Level Framework

Apply to your environment

- Identify your critical monitors
- Think about ways to subvert them
- Create checks for subversion
- Iterate

Questions?